IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

PAULA MAGNANI, individually and on behalf of all others similarly situated, Plaintiff, v. **ENZO BIOCHEM, INC.** and **ENZO CLINICAL LABS, INC.,** Defendants.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Paula Magnani ("Plaintiff") brings this Class Action Complaint, individually and on behalf of all others similarly situated (the "Class Members"), against Enzo Biochem, Inc. ("Enzo Biochem") and Enzo Clinical Labs, Inc. ("Enzo Clinical," and collectively with Enzo Biochem, "Enzo" or "Defendants") alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

NATURE OF CASE

1. This class action arises out of the recent, targeted cyberattack and data breach where unauthorized third-party criminals retrieved and exfiltrated personal data from Enzo's network that resulted in unauthorized access to the highly sensitive consumer data[1] of Plaintiff, and, according to Enzo, at least 2,470,000 Class Members ("Data Breach").[2] After learning of the Data Breach, Enzo waited nearly two months to notify affected individuals.

[1] Enzo Biochem, Inc. SEC Filing (May 30, 2023), https://www.sec.gov/Archives/edgar/data/316253/000121390023044007/ea178836-8k_enzobiohem.htm

[2] *Id.*

2. Enzo Biochem is a leading life sciences and biotechnology company, based in New York. [3] Enzo Clinical, a wholly-owned subsidiary of Enzo Biochem, is New York-regional full service clinical reference laboratory.[4]

3. Information compromised in the Data Breach includes personally identifying information ("PII") and protected health information ("PHI") such as names, clinical test information and dates of service, and Social Security numbers (collectively, "PII" and "PHI" is "Private Information").

4. Plaintiff brings this class action lawsuit individually and on behalf of those similarly situated to address Defendants' inadequate safeguarding of Plaintiff's and Class Members' Private Information that Defendants collected and maintained.

5. Defendants maintained the Private Information in a negligent and/or reckless manner. In particular, the Private Information was maintained on Defendants' computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take steps necessary to secure Private Information from those risks left that Private Information in a vulnerable condition. In addition, the Enzo Defendants and their employees failed to properly monitor the computer network and IT systems that housed the Private Information.

[3] Enzo Biochem, Inc., About Us, https://www.enzo.com/corporate/about-us (last accessed June 25, 2023); Enzo Biochem, Inc., Home Page, https://www.enzoclinicallabs.com/ (last accessed June 25, 2023).
[4] *Id*.

6. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts and taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' Private Information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names, and giving false information to police during an arrest.

7. As a result of the Data Breach, Plaintiff and Class Members face a substantial risk of imminent and certainly impending harm. Plaintiff and Class Members have and will continue to suffer injuries associated with this risk, including but not limited to a loss of time, mitigation expenses, and anxiety over the misuse of their Private Information.

8. Even those Class Members who have yet to experience identity theft have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of Private Information, loss of privacy, and/or additional damages as described below.

9. Indeed, Defendants, themselves, encourage Class Members to spend time dealing with the Data Breach. In announcing the Data Breach, Defendants have encouraged Class Members to review correspondence and contact Defendants separately if they do not get the notice

of the Data Breach, instructing Class Members to call them on a dedicated line.[5] When Class Members do receive formal notice, Defendants instruct them to carry out a number of tasks, including reviewing their statements and credit.

10. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful conduct, and asserting claims for: (i) negligence; (ii) breach of implied contract; (iii) unjust enrichment; (iv) breach of fiduciary duty; and (v) bailment. Through these claims, Plaintiff seeks damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

THE PARTIES

11. Plaintiff Paula Magnani is a natural person, resident, and citizen of the State of New Jersey.

12. Defendants obtained and continue to maintain the Private Information of Plaintiff and owed her a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed as a result of Defendants' inadequate data security, which resulted in the Data Breach.

13. Plaintiff recalls receiving a notice letter from Defendant Enzo Clinical, stating that an unknown actor accessed and obtained certain files on the Enzo network containing her Private Information between April 4–6, 2023.

Defendants Enzo Biochem and Enzo Clinical

14. Defendant Enzo Biochem is a corporation incorporated in New York, with its

[5] Notice of Data Security Incident, https://www.enzoclinicallabs.com/Uploaded/Website-Notice.pdf (last accessed June 25, 2023).

headquarters in Farmingdale, New York. Enzo Biochem's principal place of business is 81 Executive Blvd., Suite 3, Farmingdale, New York 11735. Defendant is a citizen of the State of New York.

15. Defendant Enzo Clinical is a wholly owned subsidiary of Defendant Enzo Biochem, incorporated in New York, with its principal place of business located at 60 Executive Blvd., Farmingdale, New York 11735.

JURISDICTION AND VENUE

16. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff and at least one member of the putative Class, as defined below, are citizens of a different state than Defendants Enzo Biochem and Enzo Clinical; there are more than 100 putative class members; and, the amount in controversy exceeds $5 million exclusive of interest and costs.

17. This Court has general personal jurisdiction over Defendants because Defendants maintain their principal places of business in Farmingdale, New York, regularly conduct business in New York, and have sufficient minimum contacts in New York.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendants' principal places of business are in this District, and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

DEFENDANTS' BUSINESS

19. Founded in 1976, Enzo Biochem is a life sciences company which "lead[s] the convergence of clinical laboratories, life sciences, and intellectual property through the development of unique diagnostic platform technologies that provide numerous advantages over

previous standards." [6] Enzo Biochem conducts all business activities through three wholly owned subsidiaries, including Enzo Clinical.[7]

20. Enzo Clinical, is a wholly-owned subsidiary of Enzo Biochem which operates a full-service clinical reference laboratory and the "GoTestMeNow" Online Platform.[8] Enzo Clinical markets itself as "one of the leading regional labs in the country, as we combine the extensive testing capabilities of a large laboratory with the convenience and personalized service of a local one." [9]

21. Enzo Defendants generate approximately $100 million annual revenue.[10] Enzo trades on the New York Stock Exchange under the stock symbol ENZ. [11]

22. To obtain healthcare and related clinical laboratory services, patients, like Plaintiff and Class Members, must provide their doctors, medical professionals, or Defendants directly with highly sensitive Private Information. As part of their business, Defendants then compile, store, and maintain the Private Information they receive from patients and healthcare professionals who utilize Defendants' services. In their over 45 years of experience, Defendants have served millions of individuals, indicating that they have created and maintain a massive repository of Private Information: a particularly lucrative target for data thieves looking to obtain, misuse, or sell patient data.

---

[6] Enzo Clinical Labs, Inc., https://www.enzo.com/ (last accessed June 25, 2023).
[7] *Id.*
[8] Enzo Clinical Labs, Inc., https://www.enzoclinicallabs.com/ (last accessed June 25, 2023).
[9] *Id.*
[10] *Enzo Biochem Reports Fourth Quarter and Fiscal Year 2022 Financial Results and Provides Business Update*, GlobalNewswire (Oct. 14, 2022) https://www.globenewswire.com/en/news-release/2022/10/14/2534560/0/en/Enzo-Biochem-Reports-Fourth-Quarter-and-Fiscal-Year-2022-Financial-Results-and-Provides-Business-Update.html.
[11] Yahoo! Finance, *Enzo Biochem, Inc. (ENZ)*, https://finance.yahoo.com/quote/ENZ/ (last accessed June 23, 2023).

23. On information and belief, in the ordinary course of their business of providing medical care and services, Enzo maintains the Private Information of consumers, including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial and/or payment information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Health insurance information;
- Clinical testing information and results;
- Other information that Defendants may deem necessary to provide services and care.

24. Additionally, Defendants may receive Private Information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, patients' other doctors, patients' health plan(s), close friends, and/or family members.

25. Because of the highly sensitive and personal nature of the information Defendants acquire and store with respect to patients and other individuals, Enzo, upon information and belief, promises to, among other things: keep PHI private; comply with health care industry standards related to data security and Private Information, including HIPAA; inform consumers of their legal duties and comply with all federal and state laws protecting consumer Private Information; only

use and release Private Information for reasons that relate to medical care and treatment; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

26. As a HIPAA covered business entity (*see infra*), Enzo Clinical is required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

27. However, Enzo Defendants did not maintain adequate security to protect their systems from infiltration by cybercriminals, and they waited nearly two months to publicly disclose the Data Breach.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

Enzo Clinical is a Covered Entity Subject to HIPAA

29. Enzo Clinical is a HIPAA covered entity that provides services to patients and healthcare and medical service providers. As a regular and necessary part of its business, Enzo Clinical collects the highly sensitive Private Information of its and its clients' patients. As a covered entity, Enzo Clinical is required under federal and state law to maintain the strictest confidentiality of the patient's Private Information that it acquires, receives, and collects, and Enzo Clinical is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

30. As a covered entity under HIPAA, Enzo Clinical is required to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

31. Due to the nature of Enzo Clinical's business, which includes providing a range of clinical medical services, including storing and maintaining electronic health records, Enzo Clinical would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Enzo Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

33. Plaintiff and Class Members are or were patients, or are the executors or surviving spouses of patients, whose medical records and Private Information were maintained by, or who received health-related or other services from Enzo and directly or indirectly entrusted Enzo with their Private Information.

34. Plaintiff and Class Members relied on Enzo to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information. Plaintiff and Class Members reasonably expected that Enzo would safeguard their highly sensitive information and keep that Private Information confidential.

35. As described throughout this Complaint, Enzo did not reasonably protect, secure, or store Plaintiff's and Class Members' Private Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information Enzo maintained. Consequently, cybercriminals circumvented Enzo's security measures, resulting in a significant data breach.

THE DATA BREACH AND NOTICE LETTER

36. According to the Notice Letter Enzo provided to Plaintiff and Class Members, Enzo was subject to a ransomware attack where unauthorized parties accessed Private Information on Enzo's networks between April 4–6, 2023.[12]

37. On April 6, 2023, Enzo Defendants were alerted to unusual activity on their network. In response, according to the Notice Letter, Enzo "began an investigation with the assistance of a cybersecurity firm" and "took steps to secure our systems."[13]

38. Through Enzo's investigation, Enzo determined that "an unauthorized party accessed files on our systems" and that the files contained certain Private Information, including patients' name, date of service, and clinical test information.[14] According to Enzo's SEC disclosure, the Data Breach additionally compromised the Social Security numbers of 600,000 affected individuals.

39. Enzo waited nearly two months from the date it learned of the Data Breach and the highly sensitive nature of the Private Information impacted to publicly disclose the Data Breach

[12] *See* Notification of Data Security Incident to Plaintiff Paula Magnani, Ex. A. ("Notice Letter").
[13] See *id.*
[14] *See id.*

and notify affected individuals. For example, Plaintiff's Notice Letter is dated May 31, 2023.[15]

40. In the aftermath of the Data Breach, Enzo Defendants reportedly intend to "continue to take steps to enhance the security of our computer systems and the data we maintain."[16] In other words, Defendants admit additional security was required, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' Private Information going forward.

41. In the Notice Letter Defendants recommended that Plaintiff and Class Members "review statements you receive from your healthcare providers for accuracy and contact your providers with any questions," but offers no credit monitoring or identity theft services to the majority of the nearly 2.5 million affected individuals.[17] Although Enzo is reportedly "offering complimentary credit monitoring and identity theft protection services to those whose Social Security numbers were involved," Enzo has given no indication of the duration and extent of the services it is offering.[18]

42. According to Enzo, Plaintiff's and Class Members' Private Information was exfiltrated and stolen in the attack.

43. Enzo's accessed systems contained Private Information that was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

---

[15] *See id.*
[16] *See* Notice Letter.
[17] *See 2.5M Impacted by Enzo Biochem Data Leak After Ransomware Attack*, DARKReading (June 5, 2023), https://www.darkreading.com/attacks-breaches/2-5m-impacted-by-enzo-biochem-data-leak-after-ransomware-attack. *See also* Notice Letter.
[18] Notice of Data Security Incident, https://www.enzoclinicallabs.com/Uploaded/Website-Notice.pdf (last accessed June 25, 2023).

44. As a HIPAA covered business entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk which Enzo Clinical was aware of and which the Enzo Defendants knew they had a duty to guard against. This is particularly true because the targeted attack was a ransomware attack.[19] It is well-known that healthcare businesses such as Defendants', which collect and store the confidential and sensitive PII/PHI of millions of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

45. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiff and Class Members.

46. Defendants had obligations created by HIPAA, contract, industry standards, common law, and their own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

47. Plaintiff and Class Members provided their Private Information to Enzo, either directly or indirectly, with the reasonable expectation and mutual understanding that Enzo Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

[19] *See 2.5M Impacted by Enzo Biochem Data Leak After Ransomware Attack*, DARKReading (June 5, 2023), https://www.darkreading.com/attacks-breaches/2-5m-impacted-by-enzo-biochem-data-leak-after-ransomware-attack.

48. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Enzo assumed legal and equitable duties and knew, or should have known, that they were responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

49. Due to Enzo's inadequate security measures and Enzo's delayed notice to victims, Plaintiff and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

The Data Breach was a Foreseeable Risk of which Defendants were on Notice

50. As a covered entity handling medical patient data, Enzo's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the Data Breach.

51. At all relevant times, Enzo knew, or should have known that Plaintiff's and Class Members' Private Information was a target for malicious actors. Despite such knowledge, Enzo failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' Private Information from cyberattacks that Enzo should have anticipated and guarded against.

52. In light of high profile data breaches at other health care providers, Defendants knew or should have known that their electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

53. These data breaches have been a consistent problem for the past several years, providing Defendants sufficient time and notice to harden their systems and engage in better, more comprehensive cybersecurity practices.

54. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company, Protenus, found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[20]

55. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[21]

56. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

57. Indeed, cyberattacks against the healthcare industry have been common for over eleven years with the FBI warning as early as 2011 that cybercriminals were "advancing their

[20] *2022 Breach Barometer*, PROTENUS, https://blog.protenus.com/key-takeaways-from-the-2022-breach-barometer (last visited May. 7, 2023).
[21] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available at: https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited May. 7, 2023).

abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[22]

58. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[23] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[24] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[25]

59. Cyberattacks on medical systems, like Defendants', have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[26]

60. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he

---

[22] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.
[23] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.") (last visited May. 7, 2023).
[24] *Id.*
[25] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.
[26] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents." [27]

61. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[28] In this case, Enzo stored the records of *millions* of patients.

62. Private Information, like that stolen from Enzo, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[29]

63. Indeed, cybercriminals are also monetizing encrypted data by saving it until decryption methods are developed, at which point the data will be combined with the rest of the "fullz." This practice is well-known among entities actively monitoring for such risks, as Defendants should reasonably have been doing.

64. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of

[27] The HIPAA Journal, *Editorial: Why Do Criminals Target Medical Records* (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records.
[28] See *id.*
[29] See *id*.

the full monetary value of the consumer's transaction with the company.

65. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[30]

66. Enzo was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[31]

67. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[32]

68. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiff and Class Members.

---

[30] *See* Maria Henriquez*, Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

[31] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820 (last visited May 7, 2023).

[32] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED.ASS'N (Oct 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

69. The U.S. Department of Health and Human Services and the Office of Consumer Rights urges the use of encryption of data containing sensitive personal information. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information privacy, stated in 2014 that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[33]

70. As a HIPAA covered entity, Enzo Clinical should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

Defendants Fail to Comply with FTC Guidelines

71. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

72. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[34] The guidelines also recommend that businesses use an intrusion detection

[33] Susan D. Hall, *OCR levies $2 million in HIPAA fines for stolen laptops*, Fierce Healthcare (Apr. 23, 2014), https://www.fiercehealthcare.com/it/ocr-levies-2-million-hipaa-fines-for-stolen-laptops.

[34] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Oct.

system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[35]

73. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

74. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

75. These FTC enforcement actions include actions against healthcare providers and partners like Defendants. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[35] *Id*.

76. Defendants failed to properly implement basic data security practices.

77. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

78. Defendants were at all times fully aware of their obligation to protect the Private Information of customers and patients. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Fail to Comply with Industry Standards

79. As shown above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

80. Several best practices have been identified that at a minimum should be implemented by healthcare service providers like Defendants, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limitations on which employees can access sensitive data.

81. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

82. On information and belief, Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including

without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

83. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber incident and, ultimately, causing the Data Breach.

Defendants' Conduct Violates HIPAA Obligations to Safeguard Private Information

84. As a clinical laboratory, and by handing medical patient data, Enzo Clinical is, and so acknowledges that it is, a covered entity under HIPAA (45 C.F.R. § 160.103) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

85. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

86. Enzo is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[5] *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

87. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

88. HIPAA covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

89. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

90. A Data Breach such as the one Defendants experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40

91. The Data Breach resulted from a combination of insufficiencies that demonstrate Enzo failed to comply with safeguards mandated by HIPAA regulations.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

92. Cyberattacks and data breaches at health care companies like Defendants' are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

93. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[36]

94. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with a deterioration in timeliness and patient outcomes, generally.[37]

95. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[38]

96. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate the pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social

[36] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[37] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019), *available at* https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[38] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf.

engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

97. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[39]

98. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

99. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[39] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited May 7, 2023).

100. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[40]

101. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

102. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

103. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

104. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

[40] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

105. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

106. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts, or the accounts of deceased individuals for whom Class Members are the executors or surviving spouses, for many years to come.

107. Private Information can sell for as much as $363 per record according to the Infosec Institute.[41] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

108. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[42] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[43] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

---

[41] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[42] *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf.
[43] *Id*.

109. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

110. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[44]

111. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[45]

112. Medical information is especially valuable to identity thieves.

113. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[46]

114. Drug manufacturers, medical device manufacturers, clinical laboratories, hospitals, and other healthcare service providers often purchase PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims

---

[44] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[45] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[46] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Apr. 6, 2023).

themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

115. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

116. For this reason, Defendants knew or should have known about these dangers and strengthened their data and email handling systems accordingly. Defendants were on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendants failed to properly prepare for that risk.

117. Defendants placed themselves in a position where they owed a duty to Plaintiff and Class Members by virtue of the sensitivity of the data that they collected. Indeed, because of Defendants, Plaintiff and Class Members were placed in a worse position than they would have been had Defendants not collected and maintained their data. Defendants knew the risk that they created and, accordingly, were in the best position to protect Plaintiff and Class Members by virtue of the special relationship that they created with them.

DEFENDANTS' DATA BREACH

118. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' and customers' Private Information;

c. Failing to properly monitor their own data security systems for existing

intrusions;

d. Failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;

e. Failing to train their employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R.

§ 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by their workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of their workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

p. Failing to adhere to industry standards for cybersecurity as discussed above; and

q. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' Private Information.

119. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access Enzo's computer network and systems for multiple days which contained unsecured and unencrypted Private Information.

120. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendants.

Plaintiff's and Class Members' Damages

121. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiff and Class Members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not the rest of their lives. Yet, to date, Defendants have not so much as offered to provide the majority of victims of the Data Breach with limited subscriptions to fraud and identity monitoring services. Defendants have done nothing to compensate Plaintiff or Class Members for many of the injuries they have already suffered. Defendants have not demonstrated any efforts to prevent additional harm from befalling Plaintiff and Class Members as a result of the Data Breach.

122. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

123. Plaintiff's and Class Members' names, clinical test information, dates of service, and Social Security numbers were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendants' computer system(s).[47]

124. Since being notified of the Data Breach, Plaintiff has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

[47] *See 2.5M Impacted by Enzo Biochem Data Leak After Ransomware Attack*, DARKReading (June 5, 2023), https://www.darkreading.com/attacks-breaches/2-5m-impacted-by-enzo-biochem-data-leak-after-ransomware-attack.

125. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring her accounts for fraudulent activity.

126. Plaintiff's and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

127. As a direct and proximate result of Defendants' conduct, Plaintiff's and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

128. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

129. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

130. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on Plaintiff's and Class Members' Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

131. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

132. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have

recognized the propriety of loss of value damages in related cases.

133. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Defendants and/or Defendants' healthcare partners was intended to be used by Defendants to fund adequate security of their computer system(s) and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and Class Members did not get what they paid for and agreed to.

134. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

135. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
b. Purchasing credit monitoring and identity theft prevention;
c. Placing "freezes" and "alerts" with reporting agencies;
d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;
e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

136. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

137. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

138. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

Plaintiff's Experience

139. Plaintiff provided her Private Information to her physician – who shares a medical suite with an Enzo Clinical laboratory – during a visit with her physician, in which Plaintiff had bloodwork performed by Enzo Clinical. Plaintiff's information was provided to Enzo Clinical as part of the process of obtaining medical services provided by Enzo Defendants, and Plaintiff trusted that this information would be safeguarded according to state and federal law.

140. Upon information and belief, Plaintiff was presented with standard forms to complete prior to receiving medical services that required her PII and PHI. Upon information and belief, Defendants received and maintain the information Plaintiff was required to provide to her doctors or medical professionals. Plaintiff also believes she was presented with standard HIPAA privacy notices before disclosing her Private Information to their medical provider(s).

141. Plaintiff is very careful with her Private Information. She stores any documents containing her Private Information in a safe and secure location or destroys the documents. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

142. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring her credit.

143. Plaintiff was forced to spend multiple hours attempting to mitigate the effects of the Data Breach. She will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This is time that is lost forever and cannot be recaptured.

144. Plaintiff suffered actual injury and damages from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of intangible property that Enzo obtained from Plaintiff and/or Plaintiff's doctors and medical professionals; (b) violation of her privacy rights; (c) the theft of her Private Information; (d) loss of time; (e) imminent and

impending injury arising from the increased risk of identity theft and fraud; (f) failure to receive the benefit of her bargain; and (g) nominal and statutory damages.

145. Plaintiff has also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff has also suffered anxiety about unauthorized parties viewing, using, and/or publishing information related to her Social Security number, medical records, and clinical test results.

146. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

147. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

148. Plaintiff brings this action against Enzo individually and on behalf of all other persons similarly situated ("the Class").

149. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who Enzo identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Nationwide Class").**

150. Plaintiff also proposes to represent a state subclass, defined as follows and subject to amendment as appropriate:

> **All New Jersey residents or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who Enzo identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "New Jersey Subclass").**

151. Excluded from the Classes are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

152. Plaintiff reserves the right to amend or modify the Class definitions or create additional subclasses as this case progresses.

153. Numerosity. The Members of the Classes are so numerous that joinder of all of them is impracticable. Defendants disclosed to the SEC that the Private Information of approximately 2,470,000 Class Members was compromised in Data Breach.

154. Commonality. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., HIPAA;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

g. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

h. Whether Defendants should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants breached implied contracts with Plaintiff and Class Members;

l. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether Defendants failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

155. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

156. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

157. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the data of Plaintiff and Class Members was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

158. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, to conduct this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

159. Defendants have acted on grounds that apply generally to the Classes as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

160. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the public of the Data Breach;
b. Whether Defendants owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, and safeguarding their Private Information;
c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;
e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer Private Information; and
f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

161. Finally, all members of the proposed Classes are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, the New Jersey Subclass)

162. Plaintiff re-alleges and incorporates by reference paragraphs 1–161 as if fully set forth herein.

163. By collecting and storing the Private Information of Plaintiff and Class Members, in their computer system and network, and sharing it and using it for commercial gain, Defendants owed a duty of care to use reasonable means to secure and safeguard their computer system—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

164. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

165. Plaintiff and Class Members are a well-defined, foreseeable, and probable group of patients that Defendants were aware, or should have been aware, could be injured by inadequate data security measures.

166. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and consumers, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendants were in a superior position to ensure that their systems were sufficient to protect

against the foreseeable risk of harm to Class Members from a data breach.

167. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

168. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

169. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

170. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

171. Plaintiff and Class Members have no ability to protect their Private Information that was or remains in Defendants' possession.

172. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

173. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members. In addition, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

174. Defendants' conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information and failing to provide Plaintiff and Class Members with timely notice that their sensitive Private Information had been compromised.

175. Neither Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

176. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.,* (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

177. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

178. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to nominal, compensatory, consequential, and all other damages which the Court deems appropriate in an amount to be proven at trial.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, the New Jersey Subclass)

179. Plaintiff re-alleges and incorporates by reference paragraphs 1–161 as if fully set forth herein.

180. In addition to the common law and special relationship duties alleged herein, Defendants also owed a duty to safeguard Plaintiff's and Class Members' Private Information by statute.

181. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and consumers, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendants were in a superior position to ensure that their systems were sufficient to protect

against the foreseeable risk of harm to Class Members from a data breach.

182. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

183. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

184. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

185. Defendants breached that duty, which, as discussed herein, caused Plaintiff and Class Members injuries, for which they are entitled to damages.

186. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injuries and are entitled to nominal, compensatory, consequential, and all other damages which the Court deems appropriate in an amount to be proven at trial.

COUNT III
Gross Negligence
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, the New Jersey Subclass)

187. Plaintiff re-alleges and incorporates by reference paragraphs 1–161 as if fully set forth herein.

188. Defendants knew that they were protecting the most sensitive Private Information about Plaintiff and Class Members that exists—healthcare information—which can impact anything from housing, employment, benefits, education, and other areas of an individual's life.

189. When that Private Information is compromised, the effects can be devastating to individuals, such that Defendants knew or should have known about theses effects and the need to keep this information secure and protected.

190. Defendants' failure to keep this information safe was grossly negligent, as Defendants were aware of the grave consequences of not keeping this information secure.

191. As a result of Defendants' gross negligence, Plaintiff and Class Members have suffered injury and are entitled to nominal, compensatory, consequential, and all other damages which the Court deems appropriate in an amount to be proven at trial.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, the New Jersey Subclass)

192. Plaintiff re-alleges and incorporates by reference paragraphs 1–161 as if fully set forth herein.

193. Defendants acquired and maintained the Private Information of Plaintiff and the Class that it received either directly or from its healthcare provider customers.

194. When Plaintiff and Class Members paid money and provided their Private Information to their doctors and/or healthcare providers, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with their doctors and/or healthcare professionals, their business associates, and clinical laboratories, including Defendants.

195. Plaintiff and Class Members entered into implied contracts with Defendants under which Defendants agreed to safeguard and protect such information and to timely and accurately

notify Plaintiff and Class Members that their information had been breached and compromised.

196. Plaintiff and the Class were required to deliver their Private Information to Defendants as part of the process of obtaining services provided by Defendants. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendants in exchange for services.

197. Enzo Defendants solicited, offered, and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their Private Information to Defendants, or, alternatively, provided Plaintiff's and Class Members' information to doctors or other healthcare professionals, who then provided to Defendants.

198. Defendants accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services or Plaintiff and Class Members.

199. In accepting such information and payment for services, Defendants entered into an implied contract with Plaintiff and the other Class Members whereby Defendants became obligated to reasonably safeguard Plaintiff's and the other Class Members' Private Information.

200. Alternatively, Plaintiff and Class Members were the intended beneficiaries of data protection agreements entered into between Defendants and healthcare providers.

201. In delivering their Private Information to Defendants and paying for healthcare services, Plaintiff and Class Members intended and understood that Defendants would adequately safeguard the data as part of that service.

202. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

203. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of their agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

204. Plaintiff and the Class Members would not have entrusted their Private Information to Defendants in the absence of such an implied contract.

205. Had Defendants disclosed to Plaintiff and the Class (or their physicians) that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their Private Information to Defendants (or their physicians to provide to Defendants).

206. Defendants recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

207. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Defendants.

208. Defendants breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

209. As a direct and proximate result of Defendants' conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, the New Jersey Subclass)

210. Plaintiff re-alleges and incorporates by reference paragraphs 1–161 as if fully set forth herein.

211. This count is pleaded in the alternative to breach of contract.

212. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including from money they make based upon protecting Plaintiff's and Class Members' Private Information.

213. There is a direct nexus between money paid to Defendants and the requirement that Defendants keep Plaintiff's and Class Members' Private Information confidential and protected.

214. Plaintiff and Class Members paid Defendants and/or healthcare providers a certain sum of money, which was used to fund data security via contracts with Defendants.

215. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

216. Protecting data from Plaintiff and the rest of the Class Members is integral to Defendants' business. Without their data, Defendants would be unable to provide the clinical lab testing services comprising Defendants' core business.

217. Plaintiff's and Class Members' data has monetary value, and Defendants realize this benefit when they choose to store such data.

218. Plaintiff and Class Members directly and indirectly conferred a monetary benefit on Defendants. They indirectly conferred a monetary benefit on Defendants by purchasing goods and/or services from entities that contracted with Defendants, and from which Defendants received compensation to protect certain data. Plaintiff and Class Members directly conferred a monetary benefit on Defendants by supplying Private Information, which has value, from which value Defendants derive their business value, and which should have been protected with adequate data security.

219. Defendants knew that Plaintiff and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

220. Defendants enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

221. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

222. Defendants acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

223. If Plaintiff and Class Members knew that Defendants had not secured their Private Information, they would not have agreed to provide their Private Information to Defendants (or to their physician to provide to Defendants).

224. Plaintiff and Class Members have no adequate remedy at law.

225. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in their continued possession; (vii) loss or privacy from the authorized access and exfiltration of their Private Information; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

226. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

227. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from

them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

COUNT VI
Bailment
(*On Behalf of Plaintiff and the Nationwide Class, or Alternatively, the New Jersey Subclass*)

228. Plaintiff re-alleges and incorporates by reference paragraphs 1–161 as if set fully forth herein.

229. Plaintiff and Class Members provided Private Information to Defendants—either directly or through healthcare providers and their business associates—which Defendants were under a duty to keep private and confidential.

230. Plaintiff's and Class Members' Private Information is personal property, and it was conveyed to Defendants for the certain purpose of keeping the information private and confidential.

231. Plaintiff's and Class Members' Private Information has value, and is highly prized by hackers and criminals. Defendants were aware of the risks it took when accepting the Private Information for safeguarding, and assumed the risk voluntarily.

232. Once Defendants accepted Plaintiff's and Class Members' Private Information, it was in the exclusive possession of that information, and neither Plaintiff nor Class Members could control that information once it was within the possession, custody, and control of Defendants.

233. Defendants did not safeguard Plaintiff's or Class Members' Private Information when it failed to adopt and enforce adequate security safeguards to prevent a known risk of a cyberattack.

234. Defendants' failure to safeguard Plaintiff's and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

235. As a result of Defendants' failure to keep Plaintiff's and Class Members' Private Information secure, Plaintiff and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—is appropriate.

COUNT VII
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Nationwide Class)

236. Plaintiff re-alleges and incorporates by reference paragraphs 1–161 as if fully set forth herein.

237. In light of the special relationship between Defendants and Plaintiff and Class Members, Defendants became a fiduciary by undertaking a guardianship of the Private Information to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants do store.

238. Defendants had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship with their patients, in particular, to keep secure their Private Information.

239. Defendants breached their fiduciary duty to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

240. Defendants breached their fiduciary duty to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

241. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i)

actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendants' services they received.

242. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and her counsel as Class Counsel;

b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

e) Ordering Defendants to pay for not less than five years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, nominal damages, and/or statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees, as permitted by law;

i) Pre- and post-judgment interest on any amounts awarded; and,

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: June 26, 2023

Respectfully Submitted,

/s/Steven M. Nathan

Steven M. Nathan
HAUSFELD LLP
33 Whitehall Street
Fourteenth Floor
New York, NY 10004
Tel. 646.357.1100
snathan@hausfeld.com

James J. Pizzirusso*
Amanda V. Boltax*
HAUSFELD LLP
888 16th Street N.W.
Suite 300
Washington, D.C. 20006
Tel. 202.540.7200
jpizzirusso@hausfeld.com
mboltax@hausfeld.com

Kim D. Stephens, P.S.*
Cecily C. Jordan*
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
Tel. 206.682.5600
Fax. 206.682.2992
kstephens@tousley.com
cjordan@tousley.com

Amy Keller*
DICELLO LEVITT LLP
Ten North Dearborn Street
Sixth Floor
Chicago, Illinois 60602
Tel. 312.214.7900
akeller@dicellolevitt.com

Counsel for Plaintiff

** Pro Have Vice Forthcoming*

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

PAULA MAGNANI, individually and on behalf of all others similarly situated, Plaintiff, v. **ENZO BIOCHEM, INC.** and **ENZO CLINICAL LABS, INC.,** Defendants.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

EXHIBIT A

Enzo

May 31, 2023

309 1 139220 ••••••••••••••••••••AUTO**5-DIGIT 07843
PAULA MAGNANI
[redacted]

Dear Paula Magnani,

At Enzo Clinical Labs we are committed to protecting the privacy and security of your information. We perform clinical laboratory and diagnostic services, and we are writing to inform you of an incident that involved some of your information. This letter explains the incident, measures we have taken, and some steps you may consider taking in response.

What Happened? On April 6, 2023, we identified a ransomware incident on our computer network. We immediately took steps to secure our systems and began an investigation with the assistance of a cybersecurity firm. We also notified law enforcement. The investigation determined that an unauthorized party accessed files on our systems between April 4, 2023, and April 6, 2023.

What Information Was Involved? The files contained your name, date of service, and clinical test information. Your Social Security number, billing, and payment information were **not** included.

What We Are Doing and What You Can Do. We want you to know that we take this incident very seriously. To help prevent something like this from happening in the future, we have and will continue to take steps to enhance the security of our computer systems and the data we maintain. We also recommend that you review statements you receive from your healthcare providers for accuracy and contact your providers with any questions.

For More Information. If you have any questions about this incident, please call (866) 547-1115, Monday through Friday, 9:00 a.m.–6:30 p.m. Eastern Time, excluding some major U.S. holidays.

Sincerely,

Enzo Clinical Labs